IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, v. MOHAMMED AZHARUDDIN CHHIPA, *Defendant*.	Case No.: 1:23-cr-97 (DJN)

DEFENDANT'S MOTION TO SUPPRESS
THE FRUITS OF UNDISCLOSED UNLAWFUL SEARCHES

March 2019 is the first known instance of legal process being in issued in the "re-opened" investigation against Mohammed Chhipa. That legal process was a single 18 U.S.C. §2702 request from the FBI to a Facebook account with the username Carl Johnson.[1] Yet at the time that legal process was issued, the FBI was well aware that the Carl Johnson Facebook account belonged to Mohammed Chhipa account and the FBI knew all of the information associated with it and more. At least as far back as 2013 the FBI had identified nine of Mr. Chhipa's usernames, seven of his email addresses, and three of his phone numbers. *See* Def.'s Ex 1, 2013 EC. The FBI knew of the contacts in Mr. Chhipa's phone, who he called, when, and for how long. *See* Def.'s Ex. 1, *FBI Electronic Communication*, pp. 2-4 (Aug. 6, 2013).

[1] This §2702 request itself is the subject of a separate challenge.

In 2015, the FBI was evaluating Mr. Chhipa's call patterns for the past two years. *See* Def.'s Ex. 3, *FBI Electronic Communication*, pp. 1-2 (April 10, 2015).

The government had been unlawfully searching Mr. Chhipa at least since 2008, when he was stopped at the Canadian border. From that point forward, significant amounts of Mr. Chhipa's personal data was unlawfully collected through warrantless searches. Evidence of this data collection is contained in Defense Exhibits 1-3.

A problem arose, however, when the government wanted to prosecute Mr. Chhipa. It could not prosecute him based on warrantlessly obtained evidence. Thus, in 2018, it decided to "close" its investigation. Then from 2019 to 2023, when Mohammed Chhipa was arrested, the FBI attempted to reconstruct the investigation from scratch to develop admissible information. All of this fruit had already been poisoned, however. Material gathered is poisoned even if law enforcement, years later, obtained legal processes to reconstruct what it already unlawfully possessed. "Closing" a file does not clean the taint. It must be suppressed from the government's use at trial.

Argument[2]

"[T]he exclusionary rule provides that evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure, and it reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'" *United States v. DeQuasie*, 373 F.3d 509, 519 (4th Cir. 2004) (cleaned up); *see also United States v. Hernandez*, 279 F.3d 302 (5th Cir. 2002) (prior illegal "squeezing" of defendant's luggage while in luggage compartment of bus, although unknown to defendant, taints subsequent consent because the officer "became sufficiently suspicious to engage [defendant] in conversation" in order to obtain consent to a full search of the luggage); *United States v. Jackson*, 638 F. Supp. 3d 622, 644 (E.D. Va. 2022) ("the in-custody interview is fruit of the poisonous tree, the interview will be suppressed."); *United States v. Politano*, 491 F. Supp. 456, 463 (W.D.N.Y. 1980) ("[T]he request by Agent [] to see the money could only be based upon the information obtained through the prior illegal search at the airport checkpoint by the security personnel and the Cheektowaga police officer."); LaFave, Wayne R., *Search and Seizure: A Treatise on the Fourth Amendment*, § 8.2(d) (5th ed.)(noting

[2] The argument section of this motion is almost identical, but not entirely, to the Reply on the FISA Motion, ECF No. 126. This partial redundancy is necessary because the defense is in the unfortunate position of being prohibited from knowing the true source of the underlying material derivatively used against Mr. Chhipa in his case. What is clear is that the FBI relied on far more than returns from legal processes to build its case against Mr. Chhipa. Therefore, to ensure all avenues are addressed Mr. Chhipa files the instant motion.

that exploitation of a Fourth Amendment violation "may occur by the police taking advantage of earlier illegal acts which are unknown to the consenting party and thus could not have had a coercive effect upon him").

Law enforcement cannot make the initial discovery of evidence, that is, gain knowledge of an internet service account through illegal means, and then clean the taint of that knowledge by serving a legal process on the provider of that account. *See Murray v. United States*, 487 U.S. 533, 536-37 (1988) (emphasizing that evidence is tainted when it is the direct "*or indirect result* of [an] unlawful search, up to the point at which the connection with the unlawful search becomes so attenuated as to dissipate the taint.") (emphasis added); *New York v. Harris*, 495 U.S. 14, 19 (1980) ("the indirect fruits of an illegal search or arrest should be suppressed").

As the Fourth Circuit explained in *United States v. Gaines*, 668 F.3d 170, 175 (4th Cir. 2012), "for purposes of the attenuation doctrine, the *discovery* of the evidence is the relevant event." (citing *Wong Sun v. United States*, 371 U.S. 471, 488, 487) (describing an exception to the exclusionary rule where "the connection between the lawless conduct of the police and the *discovery* of the challenged evidence has become so attenuated as to dissipate the taint") (emphasis added) (internal quotation marks and citation omitted); *United States v. Clark*, 891 F.2d 501, 505 (4th Cir.1989) ("evidence challenged on a suppression motion will not be excluded unless a causal relationship exists between that particular [Fourth Amendment] violation and the *discovery* of the evidence sought to be excluded")

(emphasis added); *United States v. Reed*, 349 F.3d 457, 464 (7th Cir.2003) ("The type of intervening events that serve to attenuate [police] misconduct are those that sever the causal connection between the illegal arrest and the *discovery* of the evidence.")(emphasis added); *see also United States v. Coleman*, 536 F. Supp. 3d 80, 84 (S.D.W. Va. 2021)("a magistrate must know something about the source of information before relying on it to find that probable cause exists.").

Simply the knowledge itself: the unlawful discovery of which account to direct the legal process, taints any material that flows from it. This reasoning applies whether the discovery is of an account, of a person, or a house. For example, law enforcement could not illicitly install a hidden camera in a person's home, learn from that footage that the occupant has a sister in whom he confides, serve a grand jury subpoena on that sister, and be able to use her information as evidence. Law enforcement is prohibited from even using derivative evidence gained from further investigation of her information. The knowledge of where to direct that grand jury subpoena was gathered unlawfully. Any material that flows from it is fatally poisoned.

This reasoning applies even if the unlawfully acquired knowledge is of a public-facing social media account. There are billions of public social media

accounts.[3] Perhaps the largest of the proverbial haystacks in which to find a needle. Conducting an unlawful search to know which one of these billions of accounts to target with legal process is still a fruit of that initial unlawful search. Using the prior example, there are billions of people on the earth roaming about in public, talking in public, driving in public, and entering their homes in public. Conducting an unlawful search to know who, among those in the community, to serve with a grand jury subpoena taints all the information that flows from it. *See United States v. Finucan*, 708 F.2d 838, 844 (1st Cir. 1983) ("Absent the illegal search, the investigators might not have known the identity of all of the third parties nor what to ask them."); *United States v. Cales*, 493 F.2d 1215, 1216 (9th Cir. 1974) (relevant question is whether "anything seized illegally, or *any leads gained from illegal activity*, tend[ed] significantly to direct the investigation toward the specific evidence sought to be suppressed.")(emphasis added).

The evidentiary tree in this case was born of a toxic seed that continued for years. The smattering of legal processes obtained a decade later does not clean the taint, nor does "closing" the investigation and reopening it a few months later. According to the FBI, this "re-opened" case was initiated by the FBI "observing" a

[3] According to the latest data, there are 5.17 billion social media *users* around the world at the start of July 2024. *See* DataReportal, *Global Social Media Statistics*, https://datareportal.com/social-media-users; *see also* Belle Wong, Top Social Media Statistics And Trends Of 2024, Forbes (May 18, 2023) (https://www.forbes.com/advisor/business/social-media-statistics/)("In 2023, an estimated 4.9 billion people use social media across the world."). If some of these users have multiple accounts, as many do, the number of *accounts* is likely double or triple that figure.

Carl Johnson Facebook account in 2019. *See e.g.* Def. Ex. 4, *Search Warrant of House* at 3-4 (Aug. 2, 2019). How the FBI even knew to observe this account is the fruit of unlawful searches it conducted on Mr. Chhipa after he was stopped at the U.S. border with Canada in 2008, and the government began to warrantlessly search his personal data to reveal identifiers, conversations, calls, contacts, and a host of other information, a fraction of which is evidenced through the heavily-redacted Exhibit 1.

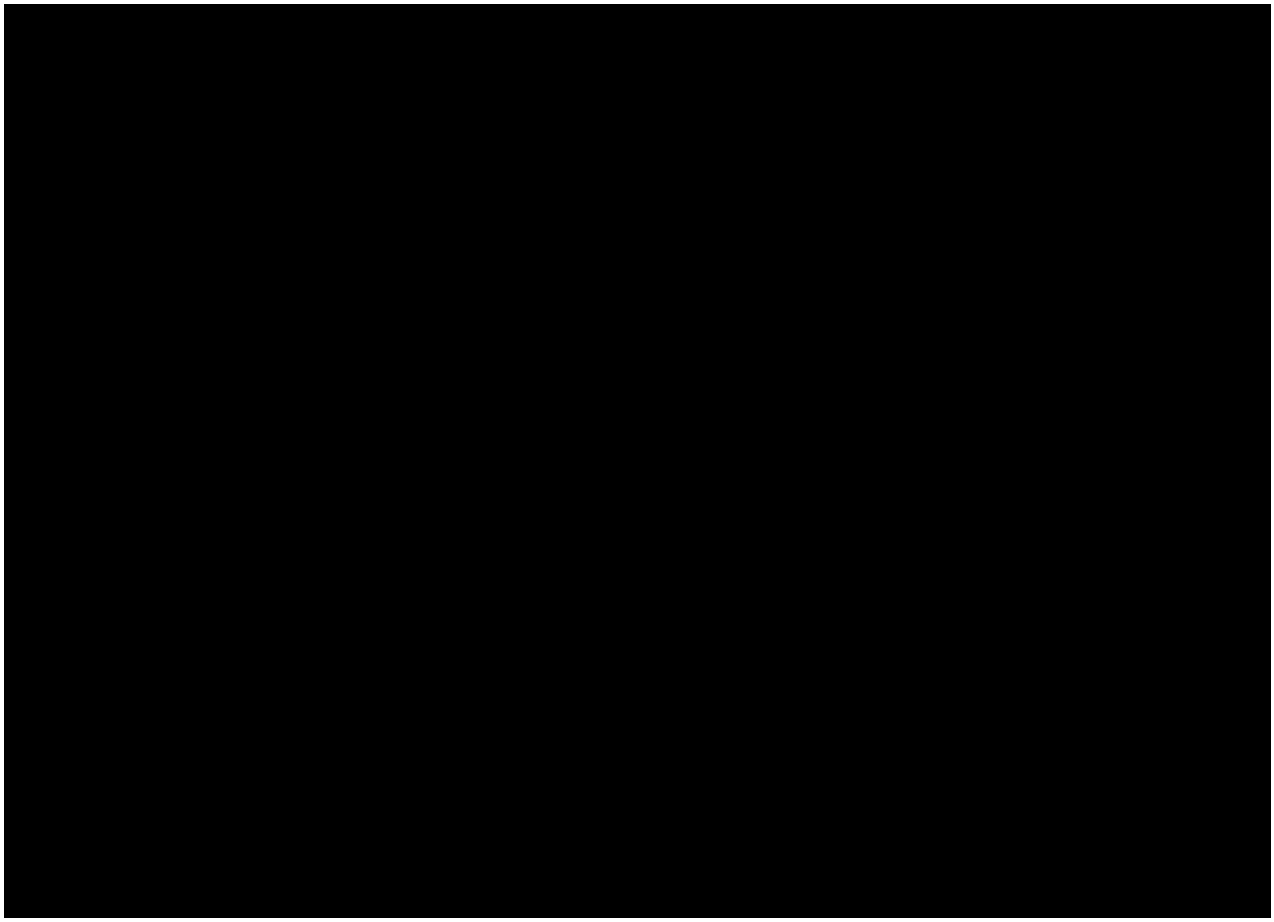
Mr. Chhipa's personal information, gathered from unlawful searches many years prior to 2019, included the Carl Johnson Facebook account. Thus, when the government states that its case began when it observed the Carl Johnson account in 2019, something triggered that observation of that account. The catalyst for that observation was the myriad of unlawful searches that had occurred prior to 2019, going back to at least as early as 2013. *See* Def. Exs. 1-3. Thus, all that flows beginning with the Carl Johnson Facebook account is still tainted by the decade of Fourth Amendment violations preceding it. *See United States v. Cordero-Rosario*, 786 F.3d 64, 77 (1st Cir. 2015) (finding relevant "whether absent the illegal search, the investigators would have known the identity of all of the third parties or what to ask them.") (citation and quotations omitted).

In *United States v. Finucan*, 708 F.2d at 843, even though there was not a clean, direct link from the unlawful search to obtaining evidence, the court of appeals affirmed the district court's suppression of evidence. The court found that "the government impermissibly exploited the illegally seized material in gathering

some of the additional evidence" because law enforcement may have relied on unlawfully seized documents "in deciding whom to interview and what to ask, and that the documents were taken to the interviews." *Id.* The court explained that the law enforcement officers "testified that the seized documents became comingled with the other evidence in the files and were not treated separately during the course of the later investigation." [4]

In this case, there are concrete examples of the way in which the decade of undisclosed, unlawful searches has fatally poisoned the evidence in this case. *First,* as of at least 2013, the FBI already knew that the Carl Johnson Facebook account was linked to Mr. Chhipa. *See* Def. Ex. 1. Yet the first search warrant in this case describes, in an incredible way, how the FBI connected the dots between the Carl Johnson account and Mohammed Chhipa. It states:

[4] There is one category of evidence that may have been independently derived; the three-way chat messages between Mr. Chhipa, ISIS MEMBER 1, and FBICP-3 in 2021. However, given the layers upon layers of comingled data form undisclosed searches preceding this timeframe, the heavy redactions, and volumes of data, it remains the government's burden to show that this material was developed entirely independently from the earlier investigation.



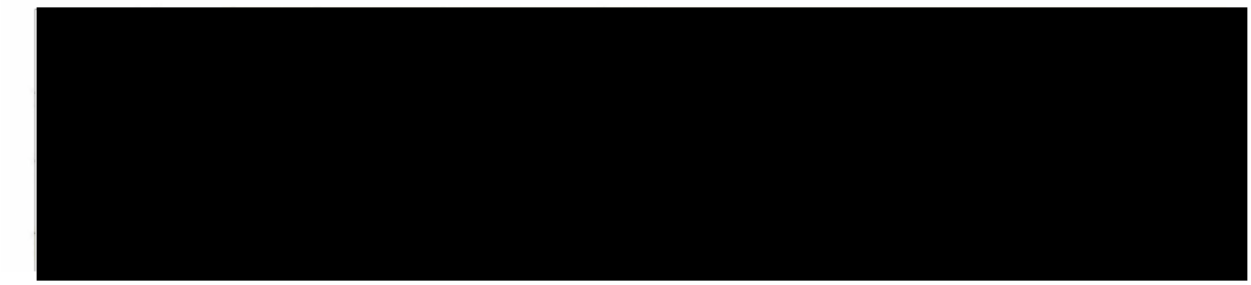
Def.'s Ex. 4 at 4.

In other words, when swearing out the search warrant to search Mr. Chhipa's house, the FBI asked this Court to believe that it linked the Carl Johnson Facebook account to Mohammed Chhipa because in a conversation the user of that account referred to *part* of a *middle name* and referenced the *entire Northern Virginia area* as the place where he lived.

Of course this is not how the Carl Johnson account was determined to be Mr. Chhipa. It would be impossible to identify someone in this way. It was determined to be Mr. Chhipa through prior undisclosed, unlawful searches at least as far back as 2013. *See* Def. Ex. 1. These searches are presumed unlawful because if they were

lawful, the FBI would have just provided the material associated with them, and also would not have gone through the trouble of creating the strained, implausible explanation as to how it connected the Carl Johnson Facebook account to Mohammed Chhipa.

Third, just days later, according to a search warrant for nine Facebook accounts:



Def. Ex. 5, *Search Warrant for Nine Facebook Accounts* at 6 (Aug. 8, 2019).

Thus, here the government's unlawful search initiated "observation" of the Carl Johnson account. The previously unlawfully collected information linked the Carl Johnson account to Mohammed Chhipa. But for these two unlawful events, law enforcement would have had no reason to query a phone number associated with Mr. Chhipa which then led to another Facebook account.

The same logic applies to two other Facebook accounts, in which the FBI states:

Id.

Without the unlawful search that generated the "observation" of the Carl Johnson account, the OCE would not have been observing the [redacted] account. Likewise, for the [redacted], but for the unlawful search connecting Mohammed Chhipa to the Carl Johnson account, the FBI would have had no reason to issue a grand jury subpoena to Google for all accounts associated with Mohammed Chhipa's phone number.

Fourth, this same search warrant for nine Facebook accounts implies that another Facebook account was discovered on March 28, 2019. It states that the account was "observed," with no indication as to why the FBI would suddenly chose to observe this account. It also makes the farfetched claim that the FBI connected

the dots to Mr. Chhipa through noticing that it began contacting Facebook friends of the Carl Johnson account:

Id.

In reality, the FBI was already aware of this moniker and its connection to Mr. Chhipa from a prior undisclosed search involving telegram on an unknown date:

Def. Ex 6, *FBI Electronic Communication* at 2 (July 2, 2019).

Fifth, both search warrants for Mr. Chhipa's residence and nine social media accounts state:

Def.'s Ex. 4 at 5; Def.'s Ex. 5 at 8.

This §2703 order for azharc27@gmail.com is for an email address that the government would not have known about based on the information that had been

returned from legal processes in the "re-opened" investigation up to that point. Indeed, when examining the application and order for the §2703(d) request, (Def.'s Ex. 7) it does not even *attempt* to link the email address to Carl Johnson or Mohamad Chhipa. It recites language posted from the Carl Johnson account, states the language is extremist, and then baldly asks for information from a seemingly random email account – with zero connection to "Carl Johnson." The return on that §2703(d) order is a fruit of unlawful searches which was then used as probable cause to obtain other fruits.

Fifth and finally, in its August 8, 2019 application for a search warrant for nine Facebook accounts, the FBI relies on prior unlawful searches to establish probable cause and discover other links and other accounts, stating as part of its probable cause process that "the FBI queried its holdings":

Def. Ex. 5 at 7.

Thus, no matter how direct a link the government can draw between one piece of evidence and a legal process, that evidence is still a fruit of the poisonous tree, just several steps farther back. These are merely the few examples of contaminated evidence that the defense has been able to obtain sifting through

terabytes of heavily redacted material, blindfolded by CIPA Section 4, with years less time than the law enforcement agents. The true contamination runs deep and wide, and like most things, begins at the beginning.

Conclusion

The inception of the investigation, born of unlawful searches, contaminates the fruit of the poisonous tree no matter how long the branches. All evidence derived therefrom must be suppressed.

Respectfully Submitted,
MOHAMMED CHHIPA,
By Counsel

/s/

Jessica N. Carmichael, VSB #78339
Zachary A. Deubler, VSB #90669
CARMICHAEL ELLIS & BROCK, PLLC
108 N. Alfred Street, 1st Floor
Alexandria, VA 22314
703.684.7908 (T)/703.649.6360 (F)
zach@carmichaellegal.com
jessica@carmichaellegal.com

CERTIFICATE OF SERVICE

I hereby certify that on this 20th day of September, 2024, I filed the foregoing pleading through the ECF system, which shall then send an electronic copy of this pleading to all parties in this action.

/s/
Jessica N. Carmichael